Annex E
Copy 4

~~TOP SECRET~~ -1- TICOM/I-180

HOMEWORK BY UFFZ. KELLER OF IN. 7/VI

AND WNV/CHI

Attached is a complete translation of a report by Unteroffizier Keller of Insp. 7/VI and WNF/Chi, on four types of hand systems used in Polish illicit W/T traffic. The report was written during October, 1945, and was received from G.S.I(S) Vienna via M.I.8.

Trans: W.R.L. No of pages: 16.

TICOM

30th December, 1945

DISTRIBUTION

British

D.D.I.
H.C.G.
D.D. (M.W.)
D.D. (A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

TICOM

S.A.C. (3)
Cdr. Bacon
Lt. Cdr. Manson
Major Cowan
Capt. Collins
Ticom Files (4)

U.S.

Op-20-G (4) (via Lt.Cdr.Manson)
G-2 (via Lt.Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, S.I.D. USFET
Col. Kunkel, USAAFE

(a)

A substitution Alphabet with alternative equivalents, (Substitution Table) reciphered (periodic adder)

A key word is written in a square 10 x 10 either in the centre (example 4) or in the four corners in the form of a spiral from the outside to the inside (example 1) or diagonally (example 2) and around this the alphabet and numerals from 1 to 0 until all the squares are filled in . The first ten figures of the current adder are taken as row and column indicators (example 4).

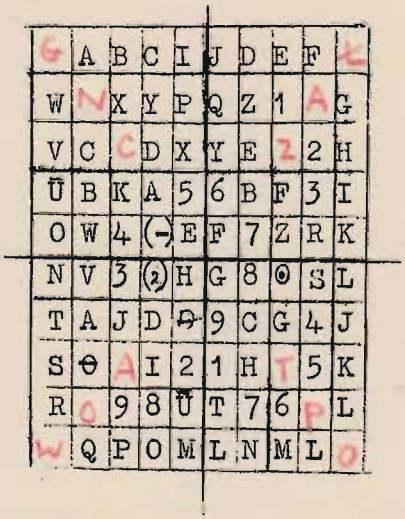
The adder is composed from the text of a book in which the letters of a line (determined by means of an indicator group) of the book in question are split up into groups of ten and the letters in such a group are numbered from 1 to 0 according to their alphabetical order (example 3).

To encipher a text the letters of the plain language text are first of all changed into numerals in accordance with the substitution table, the row indicator constitutes the first digit and the column indicator the second digit of the cipher element (example 5). The complete text having thus been turned into numerals the adder is written under it and added without carrying the tens (example 6). The message to be enciphered is usually considerably longer than the adder and in this case the adder is repeated until the complete message has been reciphered.

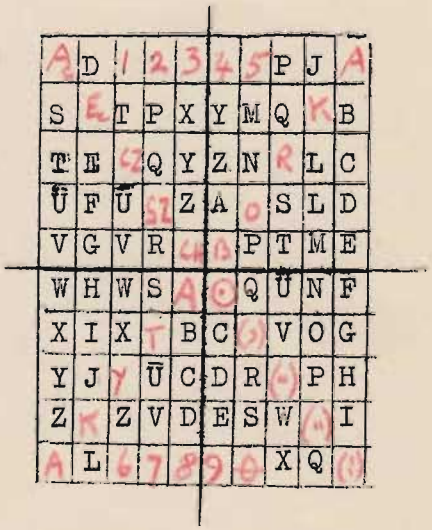
The enciphered text thus obtained is split up into groups of 5 figures each, the indicator group for the adder (page and line of the book) is written in in a position agreed upon and the indicator numerals which usually correspond to a particular substitution table are added on as the last group.

Note: In the plain langauage texts of messages in this system it is noticeable that the beginnings (and the signature) of single messages are, to a great extent, identical or similar to one another, for instance:

NR. (figures) --- NR (figures)--- DN.(figures) --- ZDN. (figures) --- DNIA (figures) --- DO (name) etc.



Example 1.



Example 2.

Example 3.

The line of the book in question reads:

lich gleichgültiges, unmenschlich, unbewegliches Gesicht blickte

lichgleich	gültigesun	menschlich	unbeweglic	hesgesicht	blickte
9715403826	2958431706	8390147625	9813045762	5284397160	1642573

Example 4:

	9	7	1	5	4	0	3	8	2	6
9	S	T	Ü	V	W	X	Y	Z	(")	1
7	R	5	6	7	8	9	Ö	A	B	2
1	Q	4	L	Ä	M	N	O	P	C	3
5	P	3	K	S	C	I	E	Q	D	4
4	O	2	J	E	K	R	Ö	R	E	5
0	N	1	I	I	A	K	(-)	S	F	6
3	M	(,)	H	M	O	W	A	T	G	7
8	Ä	Z	G	D	S	K	B	Ü	H	8
2	L	Y	F	E	I	E	C	V	I	9
6	K	X	E	Z	P	R	D	W	J	Ö

Example 5.

The following text is to be enciphered:

Nr. 127. 22.9 . DO Stem.

10 79 43 07 47 36 43 47 47 43 26 43 63 49 99 97 25 14 43
N R . 1 2 7 . 2 2 . 9 . D O S T E M .

(Enciphered from the substitution table in Example 4)

Example 6.

10 79 43 07 47 36 43 47
97 15 40 38 26 29 58 43 etc
07 84 83 35 63 55 91 80

The finished message would then commence in the following form:

(preamble) 07848 33563 55918 etc

(Trns: WRL)

(b)

Bigram Substitution Alphabet (Figure Substitution Alphabet) with short recipher (6 digit adder).

A square 30 x 30 is divided into 9 squares 10 x 10. The alphabet is written horizontally over the upper margin and vertically opposite the left-hand margin so that it is in the natural order horisontally and in a systematic but not continously alphabetical form vertically. Between the alphabets and the margins one row is kept free to enter in the row and column indicators. Figures written above and by the side of the alphabets are for the purpose of enciphering numerals, a special "figure sign" similarly written in indicates that figures and not letters are to be read (example 1).

Figures from 1 to 0 which are used in the natural order serve as row and column indicators. The beginning figures in these rows of numbers are not always the same, however, but are rather determined by means of the indicator group on each occasion (examples 2 and 3).

The 9 individual squares are likewise numbered in regular order beginning with the figure indicated by the indicator group (examples 2 and 3).

The indicator group for the row and column indicators consists of 4 figures of which one (usually the third) seems to be a dummy only, (in order to make the indicator group recognizable ?). The first figure of the indicator group denotes the figure with which the row indicator commences, the second shows the numbering of the 9 single squares and the fourth likewise denotes the column indicator (examples 2 and 3).

For reciphering 6 digit adders are used which, moreover, are different for every day of the month. The indicator group for reciphering consists of a 4 digit group which is nothing more than the date of the day and month.

Both indicator groups are reciphered, not, however, with the adders fixed for the message but (usually) with an historical year-date which stays the same in all messages (example 4).

In order to encipher a plain language text it is first of all split up into groups of 2 letters each. The row and column indicators are then written underneath the horizontal and to the right of the vertical alphabets in the cipher square, the 9 squares are also numbered, (each alphabet and also each of the 9 squares beginning with a figure chosen at random). The letters of the plain language text are now turned into figures by looking for the first letter in the vertical alphabet and the second letter in the horizontal alphabet and putting the indicator figures at the side or underneath as the case may be in place of the letters. Between the two figures thus obtained the number of the square is added which contains the intersection of the co-ordinates of these letters so that a 3 digit figure group is now produced,(example 5).

The complete plain language text being enciphered by this means the adder, determined by the date in question, is written underneath and added symbolically (i.e. without carrying the tens). The finished message is divided into 4 digit groups and the indicator groups (which are again reciphered separately with the numbers of a year) are inserted at an agreed position, (example 6).

Example 1

	1 A	1 B	1 C	2 D	2 E	2 F	3 G	3 H	3 I	4 J	4 K	4 L	5 Z	5 M	5 N	6 O	6 P	6 Q	7 R	7 S	8 T	8 U	8 V	9 W	9 X	9 Y	0 Z	0 .	0 ,	Figures
1 A																														
2 D																														
3 G																														
4 J																														
5 Z																														
6 O																														
7 R																														
8 U																														
9 X																														
0 .																														
1 B																														
2 E																														
3 H																														
4 K																														
5 M																														
6 P																														
7 S																														
8 V																														
9 Y																														
0 ,																														
1 C																														
2 F																														
3 I																														
4 L																														
5 N																														
6 Q																														
7 T																														
8 W																														
9 Z																														
0 Figures																														

Example 2.

The indicator, for instance, being:-

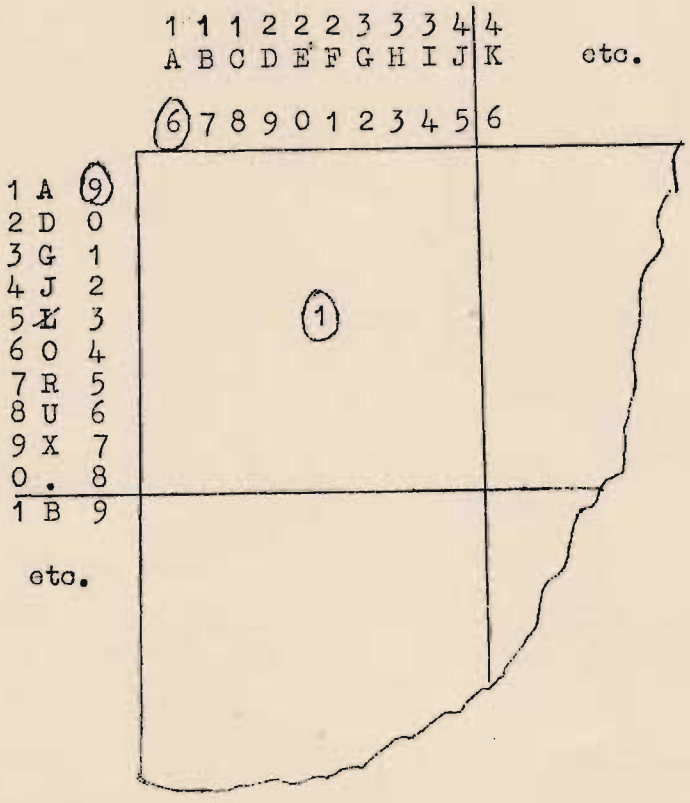
② ⑧ 4 ⑤

the complete cipher square would appear thus:

	1 1 1 2 2 2 3 3 3 4	4 4 5 5 5 6 6 6 7 7	7 8 8 8 9 9 9 0 0 0
	A B C D E F G H I J	K L Z M N O P Q R S	T U V W X Y Z . , Figures
	⑤ 6 7 8 9 0 1 2 3 4	5 6 7 8 9 0 1 2 3 4	5 6 7 8 9 0 1 2 3 4
1 A ②			
2 D 3			
3 G 4			
4 J 5			
5 Z 6	⑧	9	0
6 O 7			
7 R 8			
8 U 9			
9 X 0			
0 . 1			
1 B 2			
2 E 3			
3 H 4			
4 K 5			
5 M 6			
6 P 7	1	2	3
7 S 8			
8 V 9			
9 Y 0			
0 , 1			
1 C 2			
2 F 3			
3 I 4			
4 L 5			
5 N 6			
6 Q 7			
7 T 8	4	5	6
8 W 9			
9 Z 0			
0 Figures 1			

Example 3.

With an indicator group 9146 the cipher square would be:



Example 4.

If the indicator group was 2845 and the date 22/10 and the reciphering number for indicator groups was 1914:

	2845	2210	
	1914	1914	
the indicator groups	3759	3124	would be entered in the in the completed meassage.

Example 5.

The following text is to be enciphered:

P r z y j e c h a / e m d o l o n d y n u .

p r	z y	j e	c h	a /	e m	d o	l o	n d	y n	u .
723	060	589	242	297	328	390	550	648	029	902

(Enciphered from the cipher square in example 2).

Supposing the adder for the 22nd of each month to read : 553276 and the number with which the indicator groups are reciphered to be 1914 again:-

p r	z y	j e	c h	a ⅄	e m	d o	l o	n d	y n	u .
723	060	589	242	297	328	390	550	648	029	902
553	276	553	276	553	276	553	276	553	276	553
276	236	032	418	740	594	843	726	191	295	455

(enciphered from example 2)

The indicator groups 2845 2210
1914 1914
3759 3124

The completed message would then appear thus:-

(preamble) 2762 3603 2418 [3759] 7405 9484 3726 [3124] 1912

etc.

Trns: WRL

(c)

Bigram Substitution Alphabet (Letter Substitution Alphabet)
with Substitution Table.

A square 36 x 36 is divided into 9 individual squares 12 x 12. The alphabet is written horizontally above the upper edge and vertically by the side of the left edge in a systematic but not continuously alphabetical form in both cases (example 1).

One column is kept free between the alphabets and the edges to enter in th key word which acts on a row and column indicator. For the enciphering of numbers and other special signs, 3 further small squares 12 x 12 are provided which are written in underneath the other squares with a space of 3 or 4 lines between, (example 1).

An agreed key word (in which no letter may be repeated) acts as a row and column indicator and for the designation of the 12 individual squares. The letters of the key word with which the row and column indicators and the designation of the squares are to commence are specified by an indicator group, (examples 3 and 4).

The key word is changed at definite intervals.

For reciphering a substitution table is used in which on one side (the left) is entered the key word (beginning with the letter given by the indicator group) and on the other (the right-hand side) the normal alphabet likewise beginning with the letter given by the indicator group (example 2).

The (single) indicator group consists of 5 letters of which

the first indicates the letter with which the key-word begins when row indicator

the second indicates the letter with which the key word begins as designation of the 12 squares

the third indicates the letter with which the key word begins as column indicator

the fourth indicates the letter with which the key word begins in the substitution table

the fifth indicates the letter with which the alphabet begins in the substitution table

(examples 3 and 4).

The indicator group is not reciphered.

To encipher a plain language text it is first of all divided into groups of 2 letters each. One then enters the key word as a row and column indicator, underneath the horizontal alphabet (similarly above the 3 separate squares also) and on the right

of the vertical alphabet in the cipher square and also designates the 12 small squares, (in the case of each alphabet and of the 12 squares beginning with a letter of the key word chosen at random). The plain language letters are now converted into cipher letters by looking for the first plain language letter in the vertical alphabet and the second in the horizontal alphabet and substituting the indicator letters, at the side and below respectively, for the plain language letters.

Between the two cipher letters thus obtained the letter of the square is added which contains the intersection of the co-ordinates of the two plain language letters, so that a 3 place letter group is produced, (example 5).

The complete plain language text being enciphered by this means, the cipher text (which only consists of letters of the key word) is changed into letters of the alphabet from the substitution table.

For this purpose the key word is written on the left hand side of the substitution table and the alphabet on the right-hand side in both cases beginning with any letter of the key word or alphabet as the case may be, (example 2).

The first cipher letter is then looked for on the left-hand side of the substitution table and a letter of the alphabet on the right is substituted, after that the second letter in the same way and so on.

In this manner the whole message is enciphered and divided into 5-place groups. After the indicator group has been composed from the first letters of the column and row indicators, the designation of the squares, the key-word and the alphabet of the substitution table and inserted in the position agreed on, the message is completed, (example 6).

Example 1.

	A CZ F I L N Q SZ V X . ?	B D G J L O R T W Z , :	C E H K M P S U X Z - "
A C D F H J L M O Q S T			
V X Z . - : B CZ E G I K			
L N P R SZ U W Y Z , ? "			

	1 2 3 4 5 6 7 8 9 0	I II III IV V VI VII VIII IX X XI XII	á â é è ç
1 2 3 4 5 6 7 8 9 0			

Example 2.

If the genitive of the word pstrokacizna - "pstrokacizny" was used as the key word and the last two letters of the indicator group were ...cl, the substitution table would appear thus:-

c	l	x j
i	m	y k
z	n	z
n	o	a
y	p	b
p	q	c
s	r	d
t	s	e
r	t	f
o	u	g
k	v	h
a	w	i

Example 3.

Using the key word pstrokacizny again and if the indicator group is asoym the cipher square would appear thus: (see overleaf) and the substitution table would read:-

a	s	o	y	m
1	2	3	4	5

4	5	
(y)	(m)	y k
p	n	z l
s	o	a
t	p	b
r	q	c
o	r	d
k	s	e
a	t	f
c	u	g
i	v	h
z	w	i
n	x	j

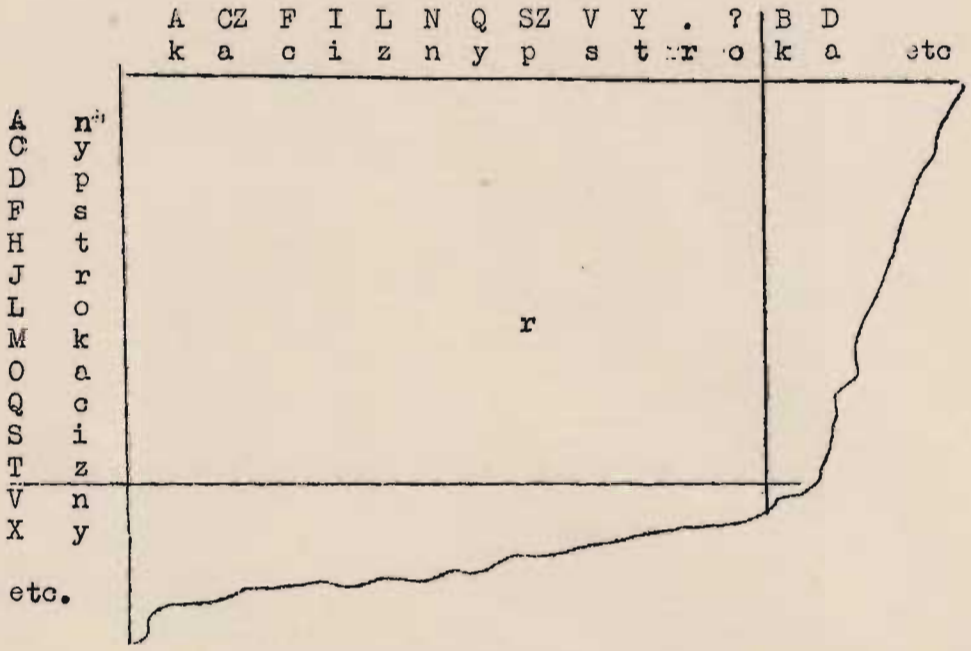
To Example 3:

	A CZ F I L N Q SZ V Y . ?	B D G J O R T W Z , :	C E H K M P S U X Z - "
	o k a c i z n y p s t r	o k a c i z n y p s t r	o k a c i z n y p s t r
A C D F H J L M O Q S T V X Z . - : B CZ E I K N P R SZ U W Y Z , ? "	s	t	r
G	o r	k	a
	o	i	z

	1 2 3 4 5 6 7 8 9 0	I II III IV V VI VII VIII IX X XI XII	á â é è ç
	o k a c i z n y p s t r	o k a ci z n y ps t r	a k a c i z n y p s t r
1 2 3 4 5 6 7 8 9 0	n	y	p

Example 4.

Indicator word as in example 3 pstrokacizny
The indicator group :- nrksb
The cipher square would then read:-



And the corresponding substitution table to it would be:-

s	b	n	z	
t	c	o	a	
r	d	p		
o	e	q		
k	f	r		
a	g	s		
c	h	t		
i	i	u		
z	j	v		
n	k	w		
y	l	x		
p	m	y		

Example 5:

The following text is to be enciphered:-

Przyjechałem do Londynu

pr	zy	je	ch	ał	em	do	lo	nd	yn	u.
iin	ios	yrk	cra	ati	tai	itz	ptz	cik	scz	yct

(enciphered from example 3).

Example 6:

The text from example 5 reciphered from the substitution table of example 3:

iin	ios	yrk	cra	ati	tai	itz	ptz	cik	scz	yct
vhj	hra	kcs	uqf	tph	bfv	vpi	zpw	uve	ogi	yub

If the 4th group were the indicator group the completed message would read:-

(preamble) vhjr akcsu qftph asqym bfvvp izpwu etc.

Trans: W.R.L.

(d)

Simple Box (without key).

The plain language text is written horizontally in a rectangle of any size (the last line which is usually incomplete is filled with dummy letters chosen at random) and read off vertically in the normal sequence of the columns from left to right. The text thus transposed is divided into groups of 5 letters each. The length and depth of the box is made known in the message by means of the first two letters whereby numbers are changed into letters by means of a substitution table (as in the following example). Note that in the message punctuation marks always appear as a combination of some other letter and q and figures (in the message) as a combination of some other letter and x, as in the following tables.

Example:

The following text is to be enciphered:-

"Beide Kennguppen werden überschlüsselt, aber nicht mit den für die Sprüche bestimmten Wurmzahlen, sondern meist mit einer geschichtlichen Jahreszahl. Diese letztere bleibt bei allen Sprüchen gleich."

Let the following be a substitution table for figures to indicate the length and depth of the box:

a	5	o	19
b	6	p	20
c	7	q	21
d	8	r	22
e	9	s	23
f	10	t	24
g	11	u	25
h	12	v	26
i	13	w	27
j	14	x	28
k	15	y	29
l	16	z	30
m	17		
n	18		

Let the following be a table for punctuation marks and figures in the message:

.	qa	1	xa
,	qb	2	xb
-	qc	3	xc
	qd	4	xd
(	qe	5	xe
)	qf	6	xf

etc.

b e i d e k e n n g r u p p e n w e r d e
n u e b e r s c h l u e s s e l t q b a b
e r n i c h t m i t d e n f u e r d i e s
p r u e c h e b e s t i m m t e n w u r m
z a h l e n q b s o n d e r n m e i s t m
i t e i n e r g e s c h i c h t l i c h e
n j a h r e s z a h l q a d i e s e l e t
z t e r e b l e i b t b e i a l l e n s p
r u e c h e n g l e i c h q a e n d e e n

The completed message would then appear thus:-

qebne pzinz reurr atjtu ienuh etc.

Trns: W.R.L.